THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **PAIGE THOMPSON'S OPPOSITION TO THE GOVERNMENT'S MOTIONS *IN LIMINE***

Paige Thompson, through counsel, opposes the government's five motions *in limine* ("MIL"), which impermissibly seek to hamstring her defense by excluding from trial evidence and argument that is relevant to the charges in the Indictment and indicative of witness bias and motive. The evidence and argument the government seeks to exclude in MIL Nos. 1, 2, 3, and 4 is relevant, probative, and admissible, and Ms. Thompson has a constitutional right to present it at trial. As for MIL No. 5, that motion is premature, and the Court can revisit the issue if Ms. Thompson elects to pursue a mental health defense.

As an additional point, the government's claim that the defense has not yet produced any reciprocal discovery is inaccurate and misleading. (*See* Dkt. No. 282 at 2.) In response to trial subpoenas, the defense received a significant volume of materials from AWS and Capital One—much of which is helpful to the defense—and directed attorneys for those entities to provide the same materials to the government as per the

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

protective orders in place. Although the defense had no obligation to do so under Federal Rule of Criminal Procedure 16 since it has not yet decided to offer *any* affirmative evidence at trial, the defense chose to provide such discovery to the government and understands Capital One and AWS attorneys have produced it directly to the government. The defense also voluntarily produced hundreds of pages of mental health records to the government for Dr. Muscatel's review.

I. ARGUMENT

Ms. Thompson's right to present evidence is governed by both the Constitution and the Federal Rules of Evidence. "Whether grounded in the Sixth Amendment's guarantee of compulsory process or in the more general Fifth Amendment guarantee of due process, the Constitution guarantees criminal defendants a meaningful opportunity to present a complete defense." *United States v. Brown*, 859 F.3d 730, 733 (9th Cir. 2017) (quoting *United States v. Stever*, 603 F.3d 747, 752 (9th Cir. 2010)). A violation of a defendant's Sixth Amendment right to present his or her defense is "structural error, and the proper remedy is a new trial." *United States v. Read*, 918 F.3d 712, 721 (9th Cir. 2019). Here, the Court's granting of any of the government's MIL would impermissibly infringe on her constitutional rights to present a defense and would not be supported by the facts or the law.

A. The Court Should Deny the Government's MIL No. 1 as Premature, Legally Unsupported, and Impermissibly Restricting Ms. Thompson's Constitutional Right to Defend Herself.

It is clear from the defense's pre-trial briefings that whether Ms. Thompson had the requisite authorization to access the AWS servers of the alleged victims, including Capital One, is central to her defense against the Computer Fraud and Abuse Act ("CFAA") charges. Put differently, as the Court found in its order denying Ms. Thompson's motion for reconsideration of her motion to dismiss Counts 2 through 8, "whether the information was public is properly resolved by the trier of fact and is

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

therefore incapable of determination before trial." (Dkt No. 271 at 4; *see also id.* at 5 ["There is therefore an unresolved question of fact regarding whether the servers were open to the 'general public.'"].)

The question of whether the information was essentially public is also relevant as to whether Ms. Thompson had the requisite intent to defraud the alleged victims. Part and parcel of determining whether Ms. Thompson's alleged access of the purported victims' AWS servers was "without authorization" is establishing how Capital One and the other purported victims configured their AWS servers and why. And part of establishing the alleged victims' reasons for configuring their AWS servers in the manner that they did—permitting public access—may involve questions regarding the cybersecurity parameters (or lack thereof), as well as cybersecurity industry standards at the time. That is relevant, probative, and admissible cross-examination that the Court should absolutely permit.

The government cites *no* case law requiring such evidence to be excluded from consideration of a CFAA charge, and the mortgage fraud case law the government cited is completely inapposite both to the CFAA charges and to the facts here that the government alleges amounts to wire fraud. More specifically, the government cites *United States v. Lindsey*, 850 F.3d 1009 (9th Cir. 2017) and *United States v. Ellison*, 704 F. App'x 616 (9th Cir. 2017), as well as cases from outside this Circuit, for the notion that victim negligence is "irrelevant." (Dkt No. 282 at 3.) But that is not precisely what the cases say, and even if they did, a mortgage fraud case has no factual similarity to a wire fraud charge based upon an alleged scheme to exploit "misconfigured" web application firewalls or WAFs. Indeed, the commentary to the Ninth Circuit Model Jury Instruction for wire fraud suggests that the *Lindsey* decision (and its progeny) are strictly limited to cases involving mortgage fraud. *See* Ninth Circuit Model Crim. Jury Instr. 15.35 (Wire Fraud), cmt.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

In any event, even assuming *Lindsey* and its progeny apply, the Ninth Circuit in *Lindsey* held that a "victim's intentional disregard of relevant information is not a defense to wire fraud" because materiality is an objective standard and a "false statement is material if it *objectively* had a tendency to influence, or was capable of influencing, a lender to approve a loan." 850 F.3d at 1015-16 (emphasis in original); *see also Ellison*, 704 F. App'x at 620 (stating that "materiality is determined objectively"). The Ninth Circuit then went on to say that the defense could absolutely attack the materiality of false statements "made in connection with securing mortgages" through "evidence of the lending standards generally applied." 850 F.3d at 1016; *see also Ellison*, 704 F. App'x at 620 (finding that defense was not precluded from arguing that a "reasonable investor" would not have been deceived).

First and foremost, as to the CFAA charges, evidence of an alleged victim's intentional disregard of relevant information is absolutely a defense because the objective touchstone is whether there is authorization. For example, if an alleged victim knew (or purposefully configured their WAF such that) a person accessing their server was not an internal user, but rather an external user, and let them access the server in any event, that would *not* be a CFAA violation because authorization would have been granted regardless of the intent of the person accessing the server. Second, *Lindsey* fully permits the defense to introduce evidence of cybersecurity industry standards and make inferential arguments from such evidence. *See* 850 F.3d at 1016-17. Third, *Lindsey* does not address, and thus does not preclude, introducing evidence of the alleged victims' prior cybersecurity vulnerabilities to dispel the government's allegation that Ms. Thompson copied "confidential business information" as opposed to attacking materiality where the entities themselves, either negligently or intentionally, do not secure the data as "confidential business information" as such data ought to be secured to invoke the law's protections. *See id.*; (Dkt. No. 131 at 8, n. 4.)

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

As the government is forced to admit, it "does not know what potential evidence of unrelated cybersecurity vulnerabilities the defense might seek to introduce, or on what basis." (Dkt. No. 282 at 3.) Making this also premature.

For all these reasons, the Court should deny this MIL.

B. The Court Should Deny Government's MIL No. 2 Because the Note is Directly Relevant to the Crimes Alleged in the Indictment.

The government's MIL No. 2 is little more than an attempt to improperly exclude evidence that does not fit—and indeed, is quite detrimental to— its narrative of the case. The handwritten note, which was delivered to an AWS employee (who is on the government's witness list) at a conference held at the downtown Seattle Sheraton Hotel on or about May 20, 2019, (USA-00015396), clearly identifies the *exact same* IP address allegedly accessed by Ms. Thompson and the *exact same* alleged vulnerability with which Ms. Thompson is criminally charged with "exploiting:" "Can Hit IMS [Instance Metadata Service] – lots of Security Credentials."[1] (Dkt. No. 282 at 6.) [redacted]

Further, although the government claims the note was "written and delivered by an unknown person," there is strong circumstantial evidence that Capital One believed Ms. Thompson authored, or otherwise authorized, the note. [redacted]

[1] The full note reads as follows:

> Open Socks Proxy
> 35.162.65.136
> Can Hit IMS – lots of
> Security Credentials

(Dkt. No. 282 at 6.)

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

[redacted] Thus, there is significant circumstantial evidence that Ms. Thompson caused the note reporting a security vulnerability in Capital One's cloud server settings to be passed to AWS at a conference in Seattle. This is not only directly relevant to whether Ms. Thompson's had the requisite criminal intent, but also relevant for the purposes of cross-examination of Capital One's witnesses.

The government's attempt to block such relevant evidence by creating a false distinction between SOCKS proxies and HTTP proxies is disingenuous. Despite their technical differences, many people—even the technologically savvy—confuse or conflate the two protocols. *See, e.g., What Is the Difference Between SOCKS and HTTP Proxies?*, GameNGuide (Mar. 1, 2022), https://www.gamenguide.com/articles/102439/20220301/what-is-the-difference-between-socks-and-http-proxies.htm ("Working with private proxies can quickly get way too confusing for most people[;] [t]here are quite a few proxy types[.]"). A simple Google search reveals dozens (if not hundreds) of articles explaining the differences between HTTP and SOCKS proxies. Additionally, programmers can utilize the two programs together by "tunnelling" a SOCKS proxy through an HTTP proxy. *See, e.g., How to Set up SSH SOCKS Tunnel for Private Browsing*, Linuxize (Mar. 19, 2019), https://linuxize.com/post/how-to-setup-ssh-socks-tunnel-for-private-browsing/; M. Holley, *How to Route Web Traffic Securely Without a VPN Using a SOCKS Tunnel*, DigitalOcean (Jan. 7, 2016), https://www.digitalocean.com/community/tutorials/ how-to-route-web-traffic-securely-without-a-vpn-using-a-socks-tunnel.

Thus, to claim, as the government does, that the entire note is irrelevant and confusing because it says "Open Socks Proxy" instead of "Open HTTP Proxy" when it

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

also identifies the very same publicly facing vulnerable IP address and alleged security vulnerability is an attempt to hide the entire forest for a single, cherry-picked tree. At most, such a picayune difference goes to the weight of the evidence, not whether it is admissible.

Lastly, that the note was passed *after* Ms. Thompson allegedly exfiltrated Capital One's data does not make it irrelevant, as claimed by the government. As already highlighted by [redacted], the evidence is relevant to Ms. Thompson's intent in allegedly accessing and exfiltrating the data and her subsequently accessing the same server on May 26*, i.e.,* to see whether Capital One had resolved the security vulnerability after it had been reported. Additionally, the date on which the note was passed is clearly within the relevant time period alleged by the government as to both the wire fraud and CFAA counts, which is from March 2019 through July 17, 2019 as to some counts, (Dkt. No. 166 at 1, 6, 8, 9) and from March 2019 through August 5, 2019 as to others. (*Id.* at 8.) Based on all these reasons, the government's MIL No. 2 should be denied.

C. The Court Should Deny Government MIL No. 3 Because the OCC Consent Order is Not Inadmissible Hearsay and is Relevant to Capital One's Bias and Motive as well as the Government's Charges Against Ms. Thompson.

The government's MIL No. 3 is yet another improper attempt to constrain Ms. Thompson's ability to effectively cross-examine Capital One witnesses. Evidence of the Office of the Comptroller of the Currency's ("OCC's") $80 million fine—and the underlying circumstances—are relevant to the bias of Capital One's witnesses. Certainly, Capital One, who has been the subject of Congressional and Department of Justice investigations, OCC fines, and civil class action lawsuits, has a vested interest in blaming Ms. Thompson. The government's apparent fear is that Ms. Thompson may be able to do the same by suggesting "that the breach was Capital One's fault, rather than

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Thompson's." (Dkt. No. 282 at 10.) But Ms. Thompson has a Sixth Amendment right to confront the witnesses against her and to confront them with evidence of their bias and motive for pointing the finger in her direction and recategorizing her as a "hacker" when they initially categorized her as a "security researcher." Capital One had, and continues to have, every incentive to want to try to refurbish its image by foisting whatever blame it could on Ms. Thompson and that is an entirely proper topic of cross-examination as to Capital One's witnesses.

Additionally, as highlighted in Ms. Thompson's response to the government's MIL No. 1 above, evidence regarding Capital One's decision to configure its servers to permit external, public access to its internal servers and industry-standard cybersecurity practices, both of which are addressed by the OCC's consent order, are admissible to establish both that Ms. Thompson did not access Capital One's servers "without authorization" under the CFAA and that she did not possess the requisite intent to defraud under the wire fraud statute.

Further, the government is simply wrong that the Consent Order is inadmissible hearsay. (Dkt. No. 282 at 10.) The Consent Order constitutes "factual findings from a legally authorized investigation" by a public office that is being subsequently utilized in a criminal case against the government; as such, it falls into the specific hearsay exception outlined in Federal Rule of Evidence 803(8)(iii) and is admissible for all purposes, including for the truth of the matter asserted. *See United States v. Gluk*, 831 F.3d 608, 614-15 (5th Cir. 2016) (finding that SEC reports of investigation and clawback complaint were public records under Rule 803(8) and admissible at trial for the truth of the matter asserted); *United States v. Riddle*, 103 F.3d 423, 430 (5th Cir. 1997) (stating that portions of OCC reports could be admissible pursuant to Rule 803(8)); *Option Res. Grp. v. Chambers Dev. Co.*, 967 F. Supp. 846, 851 (W.D. Pa.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

1996) (holding that SEC factual findings were public records and admissible pursuant to Rule 803(8)).

In sum, evidence of the OCC's Consent Order is not hearsay and is admissible to demonstrate the bias and motive of Capital One's witnesses, as well as to dispel the government's proof of "without authorization" under the CFAA and "intent to defraud" under the wire fraud statute. The government's MIL No. 3 should be denied.

D. The Court Should Deny Government MIL No. 4 Because Capital One's Civil Class Action Settlement is Admissible Pursuant to Rule 408 and Relevant to Capital One's Bias and Motive.

As with the OCC's Consent Order, Capital One's civil class action settlement is relevant for the purposes of exploring Capital One's bias and motive for redirecting blame from Capital One to Ms. Thompson. Further, Federal Rule of Evidence 408 does not preclude the admission of this evidence because that rule contains a specific exception which permits admissibility of evidence of a settlement or conduct or statements made during settlement of a claim for "proving a witness's bias or prejudice." The Court should thus deny this MIL and permit the defense to use the civil class action settlement for this purpose.

E. The Court Should Deny Government MIL No. 5 as Premature.

The government's MIL No. 5, which seeks to exclude evidence regarding Ms. Thompson's mental health issues, should be denied as premature. There can be no doubt that Ms. Thompson has had a long history of significant mental health issues and was suffering from acute mental health issues around the time of the events that will be the subject of the trial. (*See, e.g.,* Dkt No. 13 at 5, Exs. 1, 6, 7; Dkt No. 44-1 at 7-8; Dkt No. 62 at 12-13.) What is in doubt at this juncture, however, is how and whether such evidence will come in at trial. To be clear, Ms. Thompson has not decided—and is under no legal requirement to decide—prior to trial whether she intends to put on a mental condition defense. Her Federal Rule of Criminal Procedure 12.2 disclosure to

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

the government was out of an abundance of caution and her decision to put on a mental health defense will be highly dependent on how the government presents its case-in-chief.

The Court's rulings on motions *in limine* are "subject to change when the case unfolds" and the Court is always free "in the exercise of sound judicial discretion, to alter a previous *in limine* ruling." *Luce v. United States*, 469 U.S. 38, 41-42 (1984). The Court should avoid ruling pre-trial on an *in limine* motion where the basis for the motion is "a matter of conjecture." *Id.* at 42; *see Kensinger v. Craft*, No. C 11-00885 WHA, 2012 WL 2244297, at *2 (denying a motion in *limine* without prejudice because it "is yet unclear" as to how the mental health evidence would come in at trial). At this point, it is a matter of conjecture what the government's witnesses will say about Ms. Thompson's mental health and intent, and thus a denial of government's MIL No. 5 without prejudice is appropriate. The Court may, of course, revisit the issue should Ms. Thompson choose to pursue a mental health defense.

The government's citation to the non-binding case of *United States v. Pohlot*, 827 F.2d 889 (3d Cir. 1987) is not to the contrary. *Pohlot* is inapposite in that the Third Circuit was discussing the Insanity Defense Reform Act of 1984 and reviewing a trial court decision that had conflated the issue of mens rea with insanity. *See id.* at 895-97. In any event, even *Pohlot* recognizes that "[n]otions of intent, purpose and premeditation are malleable and their margins imprecise," and thus the Court can evaluate proffered mental health testimony at the time of trial "outside the presence of the jury" to determine its admissibility *or* issue a limiting instruction regarding the same. *Id.* at 906-07. The Court should thus deny the government's MIL No. 5 at this time.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

The government would not be prohibited from re-raising this motion should Ms. Thompson affirmatively notice a mental health defense after the government's case-in-chief. Ms. Thompson similarly reserves her right to raise additional objections at that time.

II. CONCLUSION

For the reasons set forth above, Ms. Thompson requests the Court deny all of the government's motions *in limine* and permit Ms. Thompson to fully and effectively confront the government's witnesses against her at trial.

DATED: June 3, 2022

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Christopher Sanders*
CHRISTOPHER SANDERS
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100